mn

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/628,729	07/28/2003	Anne Kirsten Eisentraeger	MS1-1280US	4013

22801 7590 06/28/2007
LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
06/28/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	**Application No.** 10/628,729	**Applicant(s)** EISENTRAEGER ET AL.	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5,6,9,10 and 13-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5,6,9,10 and 13-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *see att*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments, see pages 17-20, filed on 4/12/2007, with respect to the objection to the specification and the 35 USC 101 rejection of claims 1-63 have been fully considered and are persuasive as amended. The objection to the specification and the rejection under 35 USC 101 of claims 1-63 have been withdrawn. In communications filed on 4/12/2007, Applicant has amended claims 1, 2, 5, 6, 9, 10, 13, 14, 16, 22, 30-48, 50-54, 56, 58-63. Claims 1, 2, 5, 6, 9, 10, and 13-63 are presented for examination.

1.1 Applicant's remarks pages 17-20 filed on 4/12/2007 with respect to the art rejection of claims 1-12 have been fully considered but they are moot in view of a new ground of rejection. A new ground of rejection of claims 1, 2, 5, 6, 9, 10, and 13-63 is set forth below.

Allowable Subject Matter

2. The indicated allowability of claims 13-60 is withdrawn in view of the newly discovered reference(s) to Gerhard Frey, Michael Muller, and Hans-Georg Ruck; "Remark concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves" and Barreto et al "Efficient Algorithms for Pairing-Based Cryptosystems". Rejections based on the newly cited reference(s) follow.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 1/17/2007 and 5/18/2007 is being considered by the examiner.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 5, 6, 9, 10, 13-15, 29-32, 46-49, and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Non-Patent Literature to Gerhard Frey, Michael Muller, and Hans-Georg Ruck; "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems" IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 45, NO. 5, JULY 1999; Pages 1717-1719 (hereinafter **D1**) in view of Non-Patent Literature to Gerhard Frey, Michael Muller, and Hans-Georg Ruck; "Remark concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves"; Pages 865-874 (hereinafter **D2**) *(Applicant IDS)*.

As per claim 1, D1 substantially teaches a method comprising: *determining at least one Squared Tate pairing for at least one hyperelliptic curve* (see page 1719, left column first two paragraphs) showing computation of Tate pairing for a hyperelliptic curve as mentioned on (see page 1718, left column, last paragraph prior to part II). **D1** discloses using the Tate Pairing for computation of discrete logarithm which can be interpreted as a cryptographic process (see page 1718, right column, Remark 2.4 first paragraph) and further discloses that the improved Tate Pairing can be used to reduce the discrete logarithm problem for elliptic curves (see page 1719, right column, paragraph 1). **D1** suggests using the Tate pairing in cryptographic applications in which the Weil Pairing does not work (see page 1718, left column, part II, Remark 2.2) as explained in more details by Menezes et al in "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", also (Applicant's IDS). **D1** discloses wherein determining said Squared Tate pairing further includes: forming a mathematical chain for m, wherein m is a positive integer and an m-torsion element D is fixed on Jacobian of said hyperelliptic curve C (see pages 1717-1718, part I). (Page 1718, right column, last paragraph shows $m=p^k$ which meets the recitation of a mathematical chain as interpreted by Examiner). **D1** does not explicitly disclose wherein said mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain. However, **D2** in an analogous art discloses using Tate pairing for reducing the computation of discrete logarithm in the m-torsion part divisor class groups of hyperelliptic curve (see abstract). **D2** discloses "The divisor is the form A-g(P_0), where A is an effective divisor of degree g and A is given as the sum of Pi from i to g of Pi and the points Pi are rationale over a finite extension of k_0 of degree g" (page 865) and discloses " a function h on Xo such that the divisor of h is equal to A1 + A2 - A3 - gPo. Each element in Pico(Xo) has a representative of the form sum (i to g) of Pi - gPo, where Pi are points on Xo which are rational over an extension *l*o of ko of the fixed degree g" (see pages 866-867). This meets the recitation of *determining said Squared Tate pairing forming a mathematical chain for m wherein said mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain* (see D2, Results, pages 866-867 and page 869, paragraphs 2-3, and page 869. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain so as to reduce computation as suggested by D2 (see abstract). **D1** does not explicitly state *cryptographically processing selected information based on Tate Pairing*. Examiner takes official notice that elliptic curves and Tate Pairing have been very well known in the art of cryptography to be used in Public Key Cryptography and "identity-based key exchange and signature schemes" (known for secure encryption and authentication) as disclosed in several of Applicant's IDS such as Menezes' publication and Galbraith et al "Implementing Tate Pairing". Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply the concept of Frey et al as disclosed in D1 and D2 in cryptography application for cryptographically processing selected information and determining course of action in response to validation of selected information. One of ordinary skill in the art would have recognized the advantages of reducing computation in cryptosystems to implement Tate Pairing for finding groups of points on an elliptic curve to construct public key cryptosystems for identity-based key exchange and signature schemes as known in the art.

As per claim 2, D1 discloses computing Tate Pairing for a hyperelliptic curve over a field F (see pages 1717-1718, part I) that meets the recitation of *wherein said Squared Tate pairing is defined for at least one hyperelliptic curve C of genus g over a field K* (see page 1718, left column, last paragraph prior to part II), a hyperelliptic curve by definition has a genus g.

As per claims 5-6, claims 5-6 recite the same limitations as claims 1-2 respectively except for implementing the claimed method into a storage medium. **D1** discloses (page 1719, part III first paragraph) using a computer to implement the Tate Pairing. Therefore claims 5-7 are rejected on the same rationale as the rejection of claims 1-3.

As per claim 9, D1 substantially teaches an apparatus (computer) comprising memory configured to store information suitable for use with using a cryptographic process; logic operatively coupled to said memory and configured to calculate at least one Squared Tate pairing (see page 1719, part III first paragraph) for at least one hyperelliptic curve (see page 1719, left column first two paragraphs) showing computation of Tate pairing for a hyperelliptic curve as mentioned on (see page 1718, left column, last paragraph prior to part II). **D1** discloses using the Tate Pairing for computation of discrete logarithm, which can be interpreted as partially support cryptographic processing (see page 1718, right column, Remark 2.4 first paragraph) and further discloses that the improved Tate Pairing can be used to reduce the discrete logarithm problem for elliptic curves (see page 1719, right column, paragraph 1). **D1** discloses wherein determining said Squared Tate pairing further includes: forming a mathematical chain for m, wherein m is a positive integer and an m-torsion element D is fixed on Jacobian of said hyperelliptic curve C (see pages 1717-1718, part I). (Page 1718, right column, last paragraph shows $m=p^k$ which meets the recitation of a mathematical chain as interpreted by Examiner). **D1** does not explicitly disclose wherein said mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain. However, **D2** in an analogous art discloses using Tate pairing for reducing the computation of discrete logarithm in the m-torsion part divisor class groups of hyperelliptic curve (see abstract). **D2** discloses "The divisor is the form A-g(P_0), where A is an effective divisor of degree g and A is given as the sum of Pi from i to g of Pi and the points Pi are rationale over a finite extension of k_0 of degree g" (page 865) and discloses " a function h on Xo such that the divisor of h is equal to A1 + A2 - A3 - gPo. Each element in Pico(Xo) has a representative of the form sum (i to g) of Pi - gPo, where Pi are points on Xo which are rational over an extension *l*o of ko of the fixed degree g" (see pages 866-867). This meets the recitation of *determining said Squared Tate pairing forming a mathematical chain for m wherein said mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain* (see D2, Results, pages 866-867 and page 869, paragraphs 2-3, and page 869). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain so as to reduce computation as suggested by D2 (see abstract). **D1** does not explicitly state *cryptographically processing selected information based on Tate Pairing*. Examiner takes official notice that elliptic curves and Tate Pairing have been very well known in the art of cryptography to be used in Public Key Cryptography and "identity-based key exchange and signature schemes" (known for secure encryption and authentication) as disclosed in several of Applicant's IDS such as Menezes' publication and Galbraith et al "Implementing Tate Pairing". Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to apply the concept of Frey et al as disclosed in D1 and D2 in cryptography application for cryptographically processing selected information and determining course of action in response to validation of selected information. One of ordinary skill in the art would have recognized the advantages of reducing computation in cryptosystems to implement Tate Pairing for finding groups of points on an elliptic curve to construct public key cryptosystems for identity-based key exchange and signature schemes as known in the art.

As per claim 10, D1 discloses computing Tate Pairing for a hyperelliptic curve over a field F (see pages 1717-1718, part I) that meets the recitation of *wherein said Squared Tate pairing is defined for at least one hyperelliptic curve C of genus g over a field K* (see page 1718, left column, last paragraph prior to part II), a hyperelliptic curve by definition has a genus g.

As per claim 13, D1 substantially discloses determining a hyperelliptic curve E of genus g over a field F and a positive integer m (see pages 1717-1718, part I), **D1** discloses determining a Jacobian J(C) of said hyperelliptic curve E (see page 1718, part I), and evaluating tate pairing on page 1718, column 2, first five paragraphs). **D1** is silent as to wherein each element D of J(E) contains a representative of the form A-g(P_0), but suggests that computation in the case that J is the Jacobian can be used effectively using Riemann-Roch theorem (see page 1718, left column, last paragraph prior to part II). **D2** in an analogous art discloses determining a hyperelliptic curve X_0 of genus g over a field K and a positive integer m (see pages 865-866) which meets the recitation of determining a hyperelliptic curve C of genus g over a field K and a positive integer m; **D2** discloses determining a Jacobian J(C) of said hyperelliptic curve C, and wherein each element D of the curve X_0 contains a representative of the form A-g(P_0), where A is an effective divisor of degree g (see page 867, first paragraph); and discloses determining a plurality of functions $h_{i,D}$ that are iterative building blocks for the formation of a function $h_{m,D}$ in order to evaluate a Tate pairing (see page 873) that meets the recitation of determining a plurality of functions $h_{i,D}$ that are iterative building blocks for the formation of a function $h_{m,D}$ in order to evaluate v_m which is a Squared Tate pairing.

As per claim 14, the references as combined above disclose wherein said hyperelliptic curve C is over a field not of characteristic 2 (see **D2**, page 873). Claim 14 is therefore rejected on the same rationale as the rejection of claim 13 above.

As per claim 15, the references as combined above disclose wherein for at least one element D of J(C), a representative for iD will be A.sub.i-g(P.sub.0), where A.sub.i is effective of degree (see **D2**, page 867, first paragraph).

As per claim 29, the references as combined above disclose determining a Squared Tate Pairing for a hyperelliptic curves v.sub.m, for an m-torsion element D of a Jacobian J(C) and an element E of J(C), that meets the recitation of determining a Squared Tate Pairing for a hyperelliptic curves v.sub.m, for an m-torsion element D of a Jacobian J(C) and an element E of J(C), with representatives (P.sub.1)+(P.sub.2)+ . . . +(P.sub.g)-g(P.sub.0) and (Q.sub.1)+(Q.sub.2)+ . . . +(Q.sub.g)-g(P.sub.0), respectively, with each P.sub.i and each Q.sub.j on the curve C, with P.sub.i not equal to .+-.Q.sub.j for all i,j, determining that vm (D , E) := (h m ,D ((Q 1) - (- Q 1) + (Q 2) - (- Q 2) + + (Q g) - (- Q g))$^{q-1/m}$ (see **D1**, page 1718, column 2) and (**D2**, page 873). This claim is also rejected on the same rationale as the rejection of claim 16 above.

As per claims 30-32 and 46, claims 30-32 and 46 recite the same limitations as claims 13-15 and 29 respectively except for implementing the claimed method into a storage medium. **D1** discloses (page 1719, part III first paragraph) using a computer to implement the Tate Pairing. Therefore claims 30-32 and 46 are rejected on the same rationale as the rejection of claims 13-15 and 29.

As per claim 47, D1 substantially teaches an apparatus (computer) comprising memory configured to store information suitable for use with using a cryptographic process; logic operatively coupled to said memory and configured to calculate at least one Squared Tate pairing (see page 1719, part III first paragraph) for at least one hyperelliptic curve (see page 1719, left column first two paragraphs) showing computation of Tate pairing for a hyperelliptic curve as mentioned on (see page 1718, left column, last paragraph prior to part II). Claim 47 also contains the same limitations as claim 13. Claim 47 is therefore rejected on the same rationale as the rejection of claim 13.

As per claims 48-49 and 63, claims 48-49 and 63 recite the same limitations as claims 14-15 and 29 respectively except for implementing the claimed method into a claimed apparatus as disclosed in claim 47. Therefore claims 48-49 and 63 are rejected on the same rationale as the rejection of claims 14-15 and 29 and claim 47.

5. **Claims 16-28, 33-45, and 50-62** are rejected under 35 U.S.C. 103(a) as being unpatentable over Non-Patent Literature to Gerhard Frey, Michael Muller, and Hans-Georg Ruck; "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems" IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 45, NO. 5, JULY 1999; Pages 1717-1719 (hereinafter **D1**) in view of Non-Patent Literature to Gerhard Frey, Michael Muller, and Hans-Georg Ruck; “Remark concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves”; Pages 865-874 (hereinafter **D2**) *(Applicant IDS)* as applied to claim 13 and further in view of Non-Patent Literature to **Barreto et al** “Efficient Algorithms for Pairing-Based Cryptosystems” *(Applicant IDS).*

As per claim 16, D2 discloses subtraction chain and further discloses in an example on page 866 adding an inverse of (x1, y1) is represented in the form (x2, -y2) and since hyperbola is used it is implicit that if a point P=(x, y) occurs in A and y.noteq.0, then -P:=(x,-y) does not occur in A as interpreted by the Examiner (this interpretation is explained in **Barreto et al** by definition, page 4) that meets the recitation of -P denotes a point -P:=(x, -y), and wherein if a point P=(x, y) occurs in A and y.noteq.0, then -P:=(x,-y) does not occur in A. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify D1 and D2 to apply the rules as disclosed in Barreto so as to define the point P as -P:=(x, -y).

As per claim 17, the references as combined above disclose associating two polynomials a1a2 which meets the recitation of a representative A.sub.i, associating two polynomials (a.sub.i, b.sub.i) which represent a divisor (see **D2,** page 873). This claim is rejected on the same rationale as the rejection of claim 16 above.

As per claim 18, the references as combined above disclose determining D as an m-torsion element of J(C) (see **D1**, page 1718, column 2) and (see **D2**, page 873). This claim is rejected on the same rationale as the rejection of claim 16 above.

As per claim 19, the references as combined above disclose if j is an integer, then h.sub.j,D=h.sub.j,D(X) denoting a rational function on C with divisor (h.sub.j,D)=jA.sub.1-A.sub.j-((j-1)g)(P.sub.0) (see **D2**, page 873). This claim is rejected on the same rationale as the rejection of claim 16 above.

As per claim 20, the references as combined above disclose wherein D is an m-torsion divisor and A.sub.m=g(P.sub.0), and a divisor of h.sub.m,D is (h.sub.m,D)=mA.sub.1-mg(P.sub.0) (see **D2**, page 873). This claim is rejected on the same rationale as the rejection of claim 16 above.

As per claim 21, the references as combined above disclose wherein h.sub.m,D is well-defined up to a multiplicative constant (see **D2**, page 873). This claim is rejected on the same rationale as the rejection of claim 16 above.

As per claim 22, the references as combined above disclose evaluating h.sub.m,D at a degree zero divisor E on said hyperelliptic curve C, wherein E does not contain P.sub.0 and E is prime to A.sub.i. (see **D2**, page 873). This claim is rejected on the same rationale as the rejection of claim 16 above.

As per claim 23, the references as combined above disclose wherein E is prime to A.sub.i for all i in an addition-subtraction chain for m. (see **D2**, page 873). This claim is rejected on the same rationale as the rejection of claim 16 above.

As per claim 24, the references as combined above disclose wherein given A.sub.i, A.sub.j, and A.sub.i+j, further comprising determining a function u.sub.i,j such that a divisor of u.sub.i,j is (u.sub.i,j)=A.sub.i+A.sub.j-A.sub.i+j-g(P.sub.0) (see **D2**, page 866, paragraph 2 which meets the claimed limitation for instance for i=1 and j=2 and see also page 868, (examples of hyperelliptic curve). **Barreto et al** further discloses bilinearity (see pages 4 and 8). This claim is also rejected on the same rationale as the rejection of claim 16 above.

As per claim 25, the references as combined above disclose evaluating h.sub.j,D(E) for j=1 that meets the recitation of evaluating h.sub.j,D(E) such that when j=1, h.sub.1,D is 1 (see **D2**, page 873).

As per claim 26, D2 discloses wherein given A.sub.i, A.sub.j, h.sub.i,D(E) and h.sub.j,D(E), evaluating u.sub.i,j = A.sub.i+A.sub.j-A.sub.i+j-g(P.sub.0) (see **D2**, page 866, paragraph 2 which meets the claimed limitation for instance for i=1 and j=2 and see also page 868, (examples of hyperelliptic curve). See also equation on page 873 Ai in the form of ID and function iD, hi(E); it only requires routine skill in the art to use two variables from this equation to derive A.sub.i, A.sub.j, h.sub.i,D(E) and h.sub.j,D(E). **Barreto et al** further discloses bilinearity (see pages 4 and 8) and discloses evaluating f sub a+b, of P and Q (see pages 7-8, section 5) that meets the recitation of h.sub.i+j,D(E)=h.sub.i,D(E)h.sub.j,D(E)u.sub.i,j(E). This claim is also rejected on the same rationale as the rejection of claim 16 above.

As per claim 27, the references as combined above disclose determining a function (u.sub.i,j)=A.sub.i+A.sub.j-A.sub.i+j-g(P.sub.0) (see **D2**, page 866, paragraph 2 which meets the claimed limitation for instance for i=1 and j=2 and see also page 868, (examples of hyperelliptic curve). **Barreto et al** further discloses bilinearity (see pages 4 and 8). This claim is also rejected on the same rationale as the rejection of claim 16 above.

As per claim 28, the references as combined above disclose the claimed method of claim 27. **D2** discloses on pages 865-866 A.sub.i+A.sub.j-A.sub.i+j-g(P.sub.0) which meets the recitation of wherein g=2 and (u.sub.i,j)=A.sub.i+A.sub.j-A.sub.i+j-2(P.sub.0) and discloses finding the divisor between A1, A2, and A3 (see **D2,** page 866). It is apparent to one of ordinary skill in the art that using the equation A.sub.i+A.sub.j-A.sub.i+j-g(P.sub.0) of **D2** and the Cantor algorithm different values of g would satisfy if the degree of a.sub.new is greater than 2, otherwise, u.sub.i,j is determined as u.sub.i,j(X):=d(x(X)), wherein d(x) is the greatest common divisor of three polynomials (a.sub.i(x), a.sub.j(x), b.sub.i(x)+b.sub.j(x)). This claim is also rejected on the same rationale as the rejection of claim 16 above.

As per claims 33-45, claims 33-45 recite the same limitations as claims 16-28 respectively except for implementing the claimed method into a storage medium. **D1** discloses (page 1719, part III first paragraph) using a computer to implement the Tate Pairing. Therefore claims 33-45 are rejected on the same rationale as the rejection of claims 16-28.

As per claims 50-62, claims 50-62 recite the same limitations as claims 16-28 respectively except for implementing the claimed method into a claimed apparatus. Therefore claims 50-62 are rejected on the same rationale as the rejection of claims 16-28.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-Form 892).

6.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/

Patent Examiner, A.U. 2136
June 18, 2007